SLO Endpoints

Single Logout Endpoints in Metadata

This topic treats Single Logout endpoints in both IdP and SP metadata. Eventually the content on this page will be rolled into the IdP Endpoints and SP Endpoints topics.

On April 9, 2013, support for SAML2 Single Logout (SLO) endpoints in IdP metadata was introduced into the Federation Manager (FM). Support for SAML2 SLO endpoints in SP metadata was added to the FM on April 30. See the Federation Manager Release Notes for screen shots.

IdP deployments that support SLO should introduce SLO endpoints into IdP metadata with care. Here's why:

> An IdP should NOT introduce an SLO endpoint into its metadata until it is sure that all of its SP partners are properly configured for SLO. Most importantly, **SP software that is configured for SLO but does not have an SLO endpoint in its metadata will cause an error at the IdP**.

For example, consider the Shibboleth SP, which is configured for SLO out-of-the-box. As long as there are SLO endpoints in SP metadata, all is well. Otherwise the following situation can occur: Suppose an IdP introduces SLO endpoints into its metadata for the first time. If a user logs out of a federated application, and the SP is configured for SLO, the SP will automatically send an SLO request to the IdP (since the IdP now has SLO endpoints in metadata). Although the IdP is willing and able to respond to SLO, the IdP immediately fails since the SP has no SLO endpoints in its metadata.

In summary, an IdP that introduces an SLO endpoint into its metadata is inviting an SP to send a logout request. If an SP does so but does not have an SLO endpoint in metadata, an error will occur…at the IdP no less!

Consequently, all SP deployments—especially Shibboleth SP deployments—should double-check their configuration:

> IMPORTANT! **SPs that issue SAML V2.0 Single Logout requests MUST ensure that their metadata includes one or more SAML V2.0 endpoints** for receiving responses. Failure to do so will result in runtime failures for users.

An SP whose endpoints are based on multiple vhosts within a single entity descriptor should avoid SLO. A user who explicitly logs out of one vhost will necessarily be logged out of **all** vhosts, which may or may not be intended. Consequently, SLO works best for SPs with simple entity descriptors based on a single vhost.

Both front-channel and back-channel bindings are supported on SLO endpoints in metadata:

SLO Endpoints in Metadata

```
<!-- SAML V2.0 -->
<md:SingleLogoutService
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://idp.example.org/idp/profile/SAML2/Redirect/SLO"/>
<md:SingleLogoutService
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://idp.example.org/idp/profile/SAML2/POST/SLO"/>
<md:SingleLogoutService
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
    Location="https://idp.example.org/idp/profile/SAML2/SOAP/SLO"/>
```

The following SAML software is known to support the SAML2 Single Logout (SLO) Profile:

- Microsoft AD FS 2.0
- simpleSAMLphp (SOAP binding at IdP only)
- Shibboleth

If you know of other implementations that support the SAML2 SLO Profile, let us know and we'll add them to the list.